Application No.: 09/878,536
Final Office Action dated August 26, 2005
RCE Dated: January 26, 2005

AMENDMENT TO THE CLAIMS

Please amend Claims 1-7, 9-24 and 2-39, and please add claims 40-41, all as shown below. Applicant reserves the right to prosecute any originally presented claims in a continuing or future application. All pending claims are reproduced below, including those that remain unchanged.

1. (Currently Amended) A security system for allowing a client to access a protected resource or application, [[said]] the protected application or resource including an application container, the security system comprising:

an application interface mechanism for receiving an access request from a client to access [[a]] the protected application or resource, and communicating [[said]] the access request to a security service, wherein the client makes the access request on the application container, and the application container calls the security service with the access request and a callback handler;

a security service for making a decision to permit or deny [[said]] the access request, wherein the security service includes a plurality of security providers that may be plugged into the security service, and wherein the security providers use the callback handler to request context information from the application container for the access request, and wherein depending on [[the]] output from [[the]] each security provider[[s]] the security service determines [[an]] entitlements for the client to use with the protected application or resource; and

a resource interface for communicating permitted access requests to [[said]] the protected application or resource.

2. (Currently Amended) The security system of claim 1 wherein [[said]] the application interface mechanism includes an application container for reading an application deployment description and registering [[said]] the application deployment description within the security service.

3. (Currently Amended) The security system of claim 2 wherein [[said]] the application container is an Enterprise Java Beans container.

4. (Currently Amended) The security system of claim 2 wherein [[said]] the application container is a WebApp container.

5. (Currently Amended) The security system of claim 1 wherein [[said]] the security service includes a plurality of access decision mechanisms for defining an access policy and for determining a contributory decision to permit, deny, or abstain from [[said]] the access request.

6. (Currently Amended) The security system of claim 5 wherein [[said]] the security service further includes an access controller for transferring [[said]] the access request to [[said]] the plurality of access decision mechanisms, and for combining [[said]] the contributory decisions into an overall decision by the security service to permit or deny [[said]] the access request.

7. (Currently Amended) The security system of claim 5 wherein [[said]] the access decision mechanisms represent a business function related access policy.

8. (Original) The security system of claim 5 wherein access decisions may be added to the security service to reflect changes in the access policy.

9. (Currently Amended) The security system of claim 5 wherein [[said]] the access decision mechanisms are used to define [[an]] entitlements for [[said]] the client to access [[said]] the protected resource.

10. (Currently Amended) The security system of claim 5 wherein a deny or abstain by any one of [[said]] the access decision mechanisms causes the security service to deny the access request.

11. (Currently Amended) The security system of claim 5 wherein an abstain by any one of [[said]] the access decision mechanisms does not cause the security service to deny the access request.

12. (Currently Amended) The security system of claim 5 wherein [[said]] the security service further includes an audit mechanism for auditing the determinations of [[said]] the plurality of access requests.

13. (Currently Amended) The security system of claim 1 wherein [[said]] the resource interface includes an interface mechanism to pass access requests to or from a protected resource.

14. (Currently Amended) The security system of claim 13 wherein [[said]] the interface mechanism includes a Java J2EE security interface.

15. (Currently Amended) The security system of claim 13 wherein [[said]] the interface mechanism includes a security provider interface.

16. (Currently Amended) The security system of claim 13 wherein [[said]] the interface mechanism is included as a plug in in [[said]] the resource interface.

17. (Currently Amended) The security system of claim 1 wherein the security service further makes a decision on whether to permit or deny a response to [[said]] the access request from [[said]] the protected resource to [[said]] the client.

18. (Currently Amended) A method of allowing a client to access a protected application, [[said]] the application including an application container, the method comprising:

receiving at an application container an access request from a client to access a protected application;

communicating the access request from the application container to [[the]] a security service together with a callback handler;

making a decision at [[said]] the security service to permit or deny [[said access]] the access request, wherein the security service includes a plurality of security providers that may be plugged into the security service;

using the callback handler at each security provider to request context information from the application container for the access request;

determining [[an]] entitlements for the client to use with the protected application depending on [[the]] output from [[the]] each security provider[[s]]; and

communicating a permitted access request to the protected application.

19. (Currently Amended) The method of claim 18 wherein [[said]] the application interface mechanism includes an application container for reading an application deployment description and registering [[said]] the deployment description within the security service.

20. (Currently Amended) The method of claim 19 wherein [[said]] the application container is an Enterprise Java Beans container.

21. (Currently Amended) The method of claim 19 wherein [[said]] the application container is a WebApp container.

22. (Currently Amended) The method of claim 18 further comprising:

defining an access policy via a plurality of access decision mechanisms within [[said]] the security service; and,

determining at each access decision mechanism a contributory decision to permit, deny, or abstain from [[said]] the access request.

23. (Currently Amended) The method of claim 22 further comprising:

transferring via an access controller [[said]] the access request to [[said]] the plurality of access decision mechanisms, and combining [[said]] the contributory decisions into an overall decision by the security service to permit or deny [[said]] the access request.

24. (Currently Amended) The method of claim 22 wherein [[said]] the access decision mechanisms represent a business function related access policy.

25. (Original) The method of claim 22 wherein access decisions may be added to the security service to reflect changes in the access policy.

26. (Currently Amended) The method of claim 22 further comprising:

using [[said]] the access decision mechanisms to define [[an]] entitlements for [[said]] the client to access [[said]] the protected resource.

27. (Currently Amended) The method of claim 22 wherein a deny or abstain by any one of [[said]] the access decision mechanisms causes the security service to deny the access request.

28. (Currently Amended) The method of claim 22 wherein an abstain by any one of [[said]] the access decision mechanisms does not cause the security service to deny the access request.

29. (Currently Amended) The method of claim 22 further comprising:

auditing via an audit mechanism the determinations of [[said]] the plurality of access requests.

30. (Currently Amended) The method of claim 18 wherein [[said]] the step of communicating the access request includes passing access requests via an interface mechanism to or from a protected resource.

31. (Currently Amended) The method of claim 30 wherein [[said]] the interface mechanism includes a Java J2EE security interface.

32. (Currently Amended) The method of claim 30 wherein [[said]] the interface mechanism includes a security provider interface.

33. (Currently Amended) The method of claim 30 wherein [[said]] the interface mechanism is included as a plug in in [[said]] the resource interface.

34. (Currently Amended) The method of claim 18 further comprising:

making a decision on whether to permit or deny a response to [[said]] the access request from [[said]] the protected resource to [[said]] the client.

35. (Currently Amended) A method for determining [[a]] user entitlements to access protected resources in a secure environment, comprising:

receiving an access request from a user application to access a protected resource, by invoking a security service with [[said]] the access request and a callback;

determining [[a]] user entitlements to access [[said]] the protected resource, wherein [[said]] the determining includes polling a plurality of security providers that may be plugged into the security service, and wherein the security providers use a callback handler to request context information from [[the]] an application container for the access request;

making a decision at [[said]] the security service based on [[said]] the user entitlements to permit or deny [[said]] the access request; and

the steps of either

(a) communicating a permitted access request to [[said]] the protected resource, or

(b) denying a denied access request to [[said]] the protected resource.

36. (Currently Amended) The method of claim 35 wherein if [[said]] the access request is permitted [[said]] entitlements also determines a type of access available to [[the]] a user of [[said]] the protected resource.

37. (Currently Amended) The method of claim 36 wherein [[said]] the type of access includes any of view, modify, delete, or copy, any part or all of [[said]] the protected resource.

38. (Currently Amended) The method of claim 35 wherein information about [[said]] user entitlements can be communicated from a first security realm to a second security realm.

39. (Currently Amended) The method of claim 38 wherein additional information from a first security realm can be used to modify the user entitlements, prior to communicating [[said]] the information about [[said]] user entitlements from [[said]] the first security realm to [[said]] the second security realm.

40. (New) The security system of claim 1, wherein entitlements comprise at least one of business logic and functionality entitlements.

41. (New) The security system of claim 1, wherein context information comprises at least one of the identity of the protected resource or application, one or more values of access request parameters and network or internet protocol address of the client.